Afr. J. Comp. & ICT
Vol. 3, Nos.1 & 2, 2010, pp. 21 - 27
ISSN 2006-1781

THE GALOIS GROUP OF THE CHEBYSHEV POLYNOMIALS OF THE FIRST KIND OF PRIME DEGREE

'Dele Oluwade
Department of Computer Science,
Salem University,
Lokoja, Kogi State,
Federal Republic of Nigeria
Email: bamideleoluwade@computer.org

Received 2nd August, 2009

ABSTRACT

The Galois Group of a polynomial p(x) is a group associated with p(x). It is a discrete structure arising from the algebraic Galois Theory of Equations. The Galois Group provides a connection between the algebraic theories of fields and groups. There is a close relationship between the roots of a polynomial and its Galois Group, to wit, the Galois Group of a polynomial refers to a certain permutation group of the roots of the polynomial. In this paper, it is shown that the Galois group of the Chebyshev polynomials of the first kind of prime degree over the field of rationals (a field of zero characteristic) is isomorphic to the cyclic group of order two. The result is established via the concept of a splitting field.

Keywords and Phrases: Galois group, Splitting field, Chebyshev polynomials of the first kind, Cyclic group.

I. INTRODUCTION

The Galois Group of a polynomial p(x) is a group associated with p(x). It is a discrete structure arising from the Galois Theory of Equations, which is due to the French scientist, Evariste Galois (1811 – 1832). The Galois Group provides a connection between the algebraic theories of fields and groups. There is a close relationship between the roots of a polynomial and its Galois Group, to wit, the Galois Group of a polynomial refers to a certain permutation group of the roots of the polynomial [8]. Algorithms [e.g. see 6, 7] and application software (e.g. MAPLE) exist for computing the Galois Group of a polynomial.

In a much earlier work, Schur [16] derived relations for the Galois Group of the exponential Taylor polynomials and showed that:

$$G\,(K, F) = \begin{cases} A_n & \text{if } n \equiv 0 \pmod 4 \\ S_n & \text{otherwise} \end{cases}$$

where S_n is the symmetric group on n letters and A_n the alternating group of degree n. This result was re-established by Coleman [5] using the concept of p-adic Newton polygons. The Galois Groups of the generalized Puiseux expansions and of periodic points are respectively discussed in [12] and [19] whilst some results on the p – adic theory of exponential sums are presented in [17].

The Galois Group structure of the Chebyshev polynomials of the first kind over a field of characteristic p (where p is a prime) has been directly or indirectly investigated by various authors including Cohen [4], Matthew [10], Niederreiter [13] and Abhyankar [1]. In [2], it was shown that various finite classical groups can be realized as Galois Groups of specific concrete polynomials using the theorems of Cameron and Kantor. To the best of the author's knowledge, there is hitherto no published result on the Galois Group of the Chebyshev polynomials (of the first kind) over a field of zero characteristic.

In this paper therefore, the splitting field of the Chebyshev polynomials of the first kind of prime degrees over a field of zero characteristic (the rationals Q) is first deduced, and then it is shown that the Galois Group of these polynomials over Q is isomorphic to the cyclic group of order two. Joint properties of the Chebyshev polynomials of the first and second kinds can be found in [18].

II. PROPERTIES OF THE CHEBYSHEV POLYNOMIALS OF THE FIRST KIND

The Chebyshev polynomials of the first kind of degree r, T_r (x), are generally defined by [11].

$$T_r(x) = \frac{(x + \sqrt{x^2 - 1})^r + (x - (x^2 - 1)^r}{2} \qquad (2.1)$$

The polynomials also satisfy the recurrence equation [8] :

$$T_{r+1}(x) = 2x\, T_r(x) - T_{r-1}(x) \qquad (2.2)$$

and are defined in the interval [1,1]

The zeros of the polynomials are given by [9].

$$x_j^{(r)} = \text{Cos}\left(\frac{(2j-1)\pi}{2r}\right) \quad (2.3)$$

where j = 1 , 2, …, n.

Other algebraic and number theoretic properties of $T_r(x)$ include the following [3, 14]:

(i) $T_r(x)$ is irreducible over Q (the rationals) only if $r = 2^k$ where k = 0, 1, 2, …

(ii) $T_{2j+1}(x)$ is reducible over Q where j = 1, 2, ….

(iii) $T_r(T_s) = T_s(T_r)$

(iv) $T_r(T_s(x)) = T_{rs}(x)$

(v) If $r \geq 2$, then only the Chebyshev polynomials of the first kind can commute with a given $T_r(x)$

(vi) The leading term in Tr (x) is always $2^{r-1} x^r$

(vii) $|T_r(x)| \leq 1$

(viii) $T_r(x_v) = (-1)^v$

(ix) If $x \in N$ (set of natural numbers) and p is an odd prime, then $T_p(x) \equiv T_1(x) \pmod p$

It can be noted that (iii) and (iv) are respectively the commutative and semigroup property of $T_r(x)$ whilst (ix) is the Fermat's Theorem for the Chebyshev polynomials.

III. GALOIS GROUP

In this section, the main results on the Galois Group of the Chebyshev polynomials of the first kind over a field of zero characteristic, Q, is presented. The results revolve round the concept of a splitting field [8, 15].

Definition 3.1

Let F[x] be the field of polynomials in the indeterminate x and $f(x) \in F[x]$. Then a finite extension K of F is said to be a splitting field over F for f (x) if f(x) can be expressed as a product of linear factors over K but not over any intermediate field between F and K.

Remark 3.2

Given any polynomial f (x) over a fundamental field F [x], a splitting field K for f (x) over F (in which f(x) has n zeros) is always guaranteed such that $[K,F] \leq n!$ where [K,F] is the dimension of the vector space K over F.

Definition 3.3

A field F is said to be of characteristic zero if $nx \neq 0 \; \forall \; x \neq 0$, $n > 0$, where $x \in F$ and $n \in Z$ (the set of integers). If $\exists \; n > 0$ such that $nx = 0 \; \forall \; x \in F$, then F is said to be of finite characteristic.

Theorem 3.4

Let p, q be primes. Then

$$\sqrt{(x_1 + y_1\sqrt{(p^r q^s)})} \equiv x_2\sqrt{q^t} + y_2\sqrt{p}$$

where x_1, y_1, x_2, y_2 ∈ R (the set of real numbers) and r, s, t ∈ N (the set of natural numbers)

Proof

By squaring the LHS of the equation:

$x_1^2+y_1^2p^rqs+2x_1y_1\sqrt{(p^rq^s)}$

Similarly, the RHS becomes

$$x_2^4q^{2t} + y_2^4\ p + 2x_2^2y_2^2\ q^t$$

By putting $x_1 = y_2\sqrt{p}$, $y_1 = x_2^2$, $p^r = q^t$ and s = t, the result follows. □

Theorem 3.5

Let T_r (x) be the Chebyshev polynomials of the first kind of prime degree p. Then the splitting field K of T_r (x) over Q (the rationals) is

$$K = Q\sqrt{p}$$

Proof

This follows from the fact that the zeros of the polynomials are given by :

$$x_j(r) = \text{Cos}\ ((2j - 1)/2r)$$

where j = 1,2, …, n. □

Definition 3.6

The Galois Group G(K,F) of a polynomial f(x) ∈ F[x] in which K is the splitting field over F is the group of all the automorphisms of K which leaves every element of F fixed.

Theorem 3.7

Let F = Q be the fundamental field and K the splitting field of T_r (x), the Chebyshev polynomials of the first kind of prime degree. Then the Galois Group G(K,F) of $T_r(x)$ is isomorphic to the cyclic group of order 2.

Proof

By Theorem 3.4, $K = Q(\sqrt{p})$. Let σ be an automorphism of K. Now,

$$Q(\sqrt{p}) = \{ a + b\sqrt{p} : a, b \in R \}$$

And so $\sigma(\sqrt{p}) = \pm\sqrt{p}$ where R is the set of real numbers.

Suppose σ (a) = a and σ (b) = b ∀ a, b ∈ R

Then

$$\sigma(a + b\sqrt{p}) = \sigma(a) + \sigma(b\sqrt{p})$$

$$= \sigma(a) + \sigma(b)\,\sigma(\sqrt{p})$$
$$= a \pm b\sqrt{p}$$

i.e. $\sigma_1 = (a \pm b\sqrt{p}) = a + b\sqrt{p}$ and $\sigma_2\,(a + b\sqrt{p}) = a - b\sqrt{p}$

where σ_1 is the identity automorphism.

∴ $G(K,F) = \{\sigma_1, \sigma_2\}$ and so $|G(K,F)| = 2$

Hence the result, since ∃ only 1 group of order 2 up to isomorphism. □

IV. CONCLUSION

It has been shown in this paper that the Galois Group of the Chebyshev polynomials of the first kind over the field of rationals Q is isomorphic to the cyclic group of order 2 when the degree of the polynomials is prime. This result was deduced directly from a consideration of the splitting field of the polynomials over Q.

REFERENCES

1. Abhyankar, Shreeram S. (1992), ‘Galois Theory on the Line in Non-Zero Characteristic’, *Bull. Am. Math. Soc.* 27(1), 68-133.
2. Abhyankar, Shreeram S (2002), ‘Three Ways of Measuring Distance, Three Orbits, Three subdegrees, or the Great Theorems of Cameron and Kantor’, *Notices of the AMS,* 49(7), 759-769
3. Churchhouse, Robert F, (ed) (1981), *Handbook of Applicable Mathematics* Vol. III: Numerical Methods (Chief editor of series: Ledermann, Walter). John Wiley & Sons, New York.
4. Cohen, S.D. (1981), ‘The Distribution of Galois Group and Hilbert’s Irreducibility Theorem, *Proc. London Math. Soc* (3) 43, 227 – 250.
5. Coleman, Robert F. (1987), ‘On the Galois Groups of the Exponential Taylor Polnomials, ‘ *Enseign. Math* 11, Ser 33, 183 – 189.
6. Durov, N.V. (2006a), ‘Computation of the Galois Group of a Polynomial with Rational Coefficients. I’, J. *Math. Sci.* (N.Y), 134, No. 6, pp. 2511-2548.
7. Durov, N.V. (2006b), ‘Computation of the Galois Group of a Polynomial with Rational Coefficients. II’, *J. Math. Sci.* (N.Y), 136, No. 3, pp. 3880-3907.
8. Hersten I.N. (1975), *Topics in Algebra*, John Wiley & Sons, New York.
9. Lyusternik, L.A., Chervonenkis, O.A and Yanpol’s Kii, A.R. (1965), *Handbook for Computing Elementary Functions* (Transl. by Tee, G. J. and edited by Stewart, K.L.). Pergamon Press, Oxford.
10. Matthews, Rex (1982), ‘Some Generalizations of Chebyshev Polynomials and Their Induced Group Structure Over a Finite Field,’ *Acta Arith* 41, 323 – 335.
11. Mavronicolas, Marios (1998), ‘ A q-Analog of Approximate Inclusion – Exclusion, *Adv. Appl. Math*. 20, 108 – 129.
12. Morton, Patrick (1998), ‘Galois Groups of Periodic Points’, *J. Algebra 201*, 401 – 428.
13. Niederreiter, H. (1971) ‘Orthogonal systems of polynomials in finite fields’, *Proc. Am. Math. Soc.* 28(2), 415 – 422
14. Rivlin, Theodore J. (1990), *Chebyshev polynomials (From approximation theory to Algebra and Number Theory)*, John Wiley and Sons, Inc, 2nd edn.
15. Stewart, Ian (1973), *Galois Theory*, Chapman and Hall, London.
16. Schur, I. (1930), *Sitzungsber. Akad. Wiss* Berlin, 443 – 449.

17. Sperben, Steven (1986), ' On The p – adic Theory of Exponential Sums', *Am. J. Math*, 108 (2), 415 – 432.
18. Udrea, Gheorghe (2000),'A problem of Diophantus – Fermat and Chebyshev Polynomials of The First Kind', *Rev. Roumaine Math. Pures Appl* (Romania Journal of Pure and Applied Mathematics), 45(3), 531 - 535
19. Vaidya, Sanju (1997), 'Generalized Puiseux expansions and their Galois Groups', *Illinois J. Maths* 4(1), 129-141.

AUTHOR'S BIODATA

Bamidele ('Dele) Oluwade is currently a Professor of Computer Science and Dean, College of Information and Communication Technology at Salem University, Lokoja, Kogi State, Nigeria. He is a holder of a B.Sc (Mathematics) degree from the Obafemi Awolowo University, Ile-Ife, Osun State, a PGD (Computer Science) from the University of Lagos, Lagos, a M.Sc (Mathematics) from the Obafemi Awolowo University, Ile-Ife, Osun State, and a Ph.D (Computer Science) degree from the University of Ibadan, Ibadan, Oyo State. Prof. 'Dele Oluwade started his university teaching career at the Department of Mathematics, Obafemi Awolowo University, Ile-Ife, where he was a Graduate Assistant. He subsequently lectured at the Department of Computer Science, University of Ibadan and the Department of Library and Information Technology, Federal University of Technology (FUT), Minna. While at FUT Minna, he was Ag. Head FUTMINnet, Head, Department of Library and Information Technology and then Head, Department of Computer Science. During his lecturing career at the University of Ibadan, he had a brief teaching and research experience at the Department of Mathematical Sciences/Prep Year Math Program, King Fahd University of Petroleum and Minerals, Dhahran, Kingdom of Saudi Arabia. He has also had teaching and/or research experience in U.S.A, and Republic of South Africa. Prof. Oluwade is registered as an Information Technology Professional with the Computer Professionals (Registration Council of Nigeria). He is, among others, a member of the Nigeria Computer Society and American Mathematical Society, as well as a Senior Member of IEEE Computer Society, USA. He is a pioneer Disciplinary Editor (Mathematics and Computational Science) of the American Journal of Undergraduate Research, published at the University of Northern Iowa, USA, and the incumbent Chair of the Nigerian Chapter of IEEE Computer Society. His current research areas of interest include Data Compression, Design and Analysis of Algorithms, Bioinformatics (DNA computing), Digital Forensics, Human-Computer Interaction (HCI), Discrete Structures and Foundations of Computer Science. His hobbies include making enquiries into metaphysical phenomena, walking and watching indigenous movies.